GRADO DE RELACIONES LABORALES Y RECURSOS HUMANOS

Trabajo Fin de Grado

La protección de datos en el ámbito laboral y el tratamiento de los datos en Recursos Humanos

Autor/es

Daniel Pérez Molina

Director/es

Ramón Hermoso Traba

Facultad Ciencias Sociales y del Trabajo

2020

ÍNDICE

LA PROTECCIÓN DE DATOS EN EL ÁMBITO LABORAL Y EL TRATAMIENTO DE LOS DATOS EN RECURSOS HUMANOS

I. Introducción

Los datos son considerados un activo más para las empresas, pero resulta intrigante como siendo uno de los más importantes, no se les presta la atención adecuada. Estos datos pueden ser de diversos tipos: cuando se trata de datos personales hay que saber cómo deben de ser tratados, incluyendo las medidas de seguridad, para cumplir con lo establecido legalmente. Al tratarse de datos personales, hay que tener en cuenta algunos derechos inespecíficos, reconocidos en la Constitución Española, que resultan de aplicación, como el derecho a la intimidad. Desde el ámbito de las relaciones laborales se deberá de conocer cuáles son las formas de obtener datos, como tratarlos y durante cuánto tiempo.

Resulta intrigante como una práctica tan común como la recepción de *curriculum vitae* puede gestionarse de manera incorrecta por el personal a cargo de ellos, actuando como consideran más oportuno, lo que ocasiona que en ocasiones no lo hagan de la manera adecuada, llegando a cometer, sin saberlo, infracciones que pueden tener consecuencias tanto legales, económicas y de imagen empresarial. Similarmente, también pueden llegarse a producir infracciones durante el proceso de selección, lo cual se debe a que el empresario busca tener la mayor cantidad de datos para poder tomar la decisión más adecuada. Esto ocasiona que se consulte internet en busca de información, siendo muy habitual que los candidatos del proceso de selección tengan redes sociales, como podrían ser Facebook, Twitter o Instagram. Además, en el caso de que los candidatos tengan el acceso público a sus redes sociales puede conllevar que el empresario crea que puede obtener y tratar de forma ilimitada esos datos, cuando esto no es así.

La protección de datos es una materia en continuo desarrollo, ya que se encuentra estrechamente vinculada a como las personas se relacionan entre sí. Esto ocasiona que lo que hace 20 años podía otorgar una protección de datos eficaz, hoy en día sea al contrario. Por otro lado, hay que tener en cuenta que la protección de datos se encuentra estrechamente vinculada a los avances tecnológicos, los cuales han propiciado un salto desde la gestión física a la digital desde los años 90. Desde el año 2007, cuando Apple lanzó el primer Iphone, la forma de comunicarnos ha evolucionado: hoy en día gracias a los smartphones podemos mandar y recibir archivos, conectarnos a Internet y a las redes sociales, prácticamente desde cualquier lugar y momento. También ha cambiado la forma en que almacenamos los datos, permitiendo almacenar gran cantidad de datos en formato digital, (ocupando poco espacio físico), cuando antes para almacenar esos datos en soportes físicos se necesitaría gran cantidad de espacio. Este avance tecnológico hacia lo digital no viene exento de amenazas, las cuales deben tenerse

en cuenta a la hora de aplicar medidas de seguridad. En especial, la mayor amenaza que supone el dominio digital proviene de que no existen fronteras geográficas, lo cual implica que los atacantes pueden proceder de cualquier lugar del mundo.

Debido a la problemática expuesta previamente, el tema de este TFG fue elegido centrándose en el departamento de Recursos Humanos, especialmente en torno a la protección y tratamiento de datos en el ámbito laboral. Esta temática cobra especial relevancia debido a lo fundamental que es en el campo de recursos humanos y se pretende expandir la introducción a la temática adquirida durante el transcurso del Grado de Relaciones Laborales y Recursos Humanos. El uso creciente de nuevas tecnologías ha propiciado que la protección de datos sea más relevante debido al impacto que ocasiona ignorar los peligros que conlleva. Este movimiento hacia lo digital conllevó una modificación del marco legal en Europa, así como posteriormente en España, hacia nuevos derechos y obligaciones. Se estima que es crucial una mayor protección a los datos y la intimidad de los trabajadores, de forma que sus derechos queden completamente protegidos. El objetivo principal de este documento es conocer cómo afecta la legislación en protección de datos al departamento de recursos humanos y saber cómo deben de tratarse los datos.

Para la consecución de dicho objetivo, se ha dividido el trabajo en varias partes diferenciadas: La primera parte versará sobre la legislación de la Unión Europea en materia de protección de datos, tratando cual es la legislación vigente y de donde surge. A este análisis, se le añadirá una comparación diferenciando la protección legislativa en este aspecto, entre la Unión Europea y Estados Unidos de América. La segunda parte tratará sobre la legislación española, viendo su evolución histórica (hasta llegar a la ley vigente al momento de la redacción de este documento), haciendo hincapié en los derechos que puede ejercitar el afectado por el tratamiento de sus datos. Así mismo analizará cuál es el régimen sancionador en materia de protección de datos que establece la Ley Orgánica 3/2018. También analizará los nuevos derechos digitales en el ámbito laboral que establece el marco legislativo español. Esta parte finalizará con el análisis de la Agencia Española de Protección de Datos.

Finalmente, la última parte irá destinada a analizar cómo se debe tratar la protección de datos en el departamento de Recursos Humanos. Se tratarán temas como las normas internacionales ISO y sus certificaciones acerca de la protección de datos en las empresas. También se hablará sobre cómo debe de actuar el personal del departamento, prestando especial atención a tres momentos: el de selección de personal, el de vigencia de la relación laboral y el de extinción de la relación. Adicionalmente, se introducirá como debe de clasificarse

la información atendiendo a diferentes criterios y cuáles son las medidas de seguridad que se deben adoptar durante el tratamiento de datos.

Este documento concluirá con las conclusiones obtenidas tras analizar el estado y necesidades del campo.

II. Régimen jurídico de la Unión Europea

En este apartado se describe el régimen jurídico presente actualmente en la Unión Europea. La intención es ver sobre que fundamentos se encuentra la protección de datos, así como conocer cuáles son las normas de aplicación en esta materia. Además, se comparará la situación jurídica de la protección de datos entre la Unión Europea y Estados Unidos.

En la Unión Europea (Muñoz Machado, 2015) los derechos fundamentales tienen tres niveles de protección, que dependiendo de los intérpretes específicos podrán ser:

- Tribunales internos de los Estados miembros, son, por ejemplo, el Tribunal Supremo o el Tribunal Constitucional en España. Es el primer lugar al que debe de acudir alguien cuando cree que le han vulnerado un derecho fundamental.
- Tribunal de Justicia de la Unión Europea, es el lugar al que debe de acudir una persona o empresa que considera violados sus derechos fundamentales por un acto de alguna institución de la Unión Europea.
- Tribunal Europeo de Derechos Humanos, una vez que se agotan todos los recursos a nivel nacional y se sigue considerando que han vulnerado tus derechos fundamentales, podrás someter el caso a este tribunal.

En la actualidad, la protección de datos de carácter personal en la Unión Europa aparece reconocida tanto en la Carta de los Derechos Fundamentales de la Unión Europea, en su artículo 8, como en el Tratado de Funcionamiento de la Unión Europea, en su artículo 16.

Si se analiza lo que dice la Carta de los Derechos Fundamentales de la Unión Europea en su artículo 8, se ve que se limita a establecer el derecho, indicando que deben de ser tratados de modo leal, previo consentimiento del afectado o por un fundamento legítimo previsto por la ley, también debe existir un fin concreto. Además, establece dos derechos más al afectado por el tratamiento: el derecho al acceso a los datos recogidos y el derecho de rectificación.

En cuanto al Tratado de Funcionamiento de la Unión Europea, se puede ver que al igual que la Carta establece el derecho a la protección de datos de carácter personal, pero a diferencia de esta establece que el Parlamento Europeo y el Consejo establecerán las normas sobre la protección de los datos de carácter personal y normas sobre la libre circulación de los datos de carácter personal. Esta última potestad que establece es muy importante, ya que de ella surgen las normas que configuran el derecho a la protección de datos de carácter personal. La última norma surgida de esta potestad es el Reglamento (UE) 2016/679, relativo a la protección de datos de carácter personal y a la libre circulación de estos datos (RGPD), el cual moderniza la normativa europea teniendo en cuenta la rápida evolución tecnológica y la globalización. Este reglamento debe cumplirse en todos los países miembros de la Unión Europea, en España inclusive al ser

miembro, pero pese a que su aprobación fue el 14 de abril de 2016, no se aplicó hasta el 25 de mayo de 2018. Este periodo tuvo la finalidad de que las empresas, organizaciones, instituciones y organismos se adaptaran a la nueva normativa, también sirvió para que los países miembros adaptaran sus legislaciones nacionales en esta materia al nuevo reglamento, por ejemplo, España tuvo que cambiar su ley de protección de datos.

El RGPD es aplicable directamente en todos los países miembros de la Unión Europea, no necesita una transposición al ordenamiento interno de cada país, como es el caso de las Directivas. El período nombrado anteriormente, tuvo la finalidad de evitar que las leyes nacionales de cada país en esta materia pudieran contener aspectos incompatibles con el RGPD. De esta forma se dejó un período de tiempo suficiente para que los países miembros adaptarán sus ordenamientos internos. En los considerandos se exponen los motivos y objetivos del reglamento, además de afirmar en el primero que el derecho a la protección de datos personales es un derecho fundamental. Entre los motivos se encuentran:

- El incremento de intercambios de datos personales dentro de la Unión, entre operadores públicos y privados.
- La rápida evolución tecnológica y la globalización, que han conllevado un aumento significativo en el intercambio de datos personales y la magnitud de la recogida.

El objetivo, tal como se expone en el décimo considerando, es garantizar un nivel elevado y uniforme de protección, así como eliminar los obstáculos a la circulación de datos personales dentro de la Unión Europea. El nivel de protección deberá de ser equivalente en todos los países miembros.

Sin embargo, mientras en la Unión Europea existe el derecho a la protección de datos, desarrollado en el RGPD, en Estados Unidos no existe una legislación a nivel nacional, sino que cada estado[1] establece sus normas y reglas al respecto, conllevando a que existan diferentes niveles de seguridad dependiendo del estado. Por ejemplo, el 1 de enero de 2020 entró en vigor en California la primera ley de privacidad en línea de Estados Unidos (Microsoft, 2020), la cual permite que los consumidores puedan prohibir a las empresas la venta de sus datos y a su vez permitiendo que los consumidores puedan pedir la eliminación de todos sus datos.

Además, el derecho a la intimidad tiene diferentes consideraciones en la Unión Europea y en Estados Unidos, ya que mientras que en la Unión Europea es un derecho fundamental, en Estados Unidos carece de tal consideración. Y es que, *"en Estados Unidos, los privacy rights no se contemplan como un derecho fundamental, sí tienen esta consideración en la Unión Europea, lo que conlleva que, en principio, entren en colisión el derecho del empresario a controlar al trabajador, en el seno de su poder de dirección y, el derecho del trabajador a que sea respetada su esfera privada, también en el lugar de trabajo, debiendo, por tanto,*

[1] Entidades subnacionales en las que se divide Estados Unidos.

buscarse un equilibrio. No cabe duda de que, en los sistemas europeos, el control empresarial se encuentra más limitado que en Estados Unidos." (Orellana Cano, 2019, pág. 44)

III. Régimen jurídico en España

En este apartado se hablará de la evolución jurídica de la protección de datos en España, hasta llegar a la legislación vigente en el momento de realización de este trabajo. La finalidad es ver como los avances tecnológicos han ocasionado cambios legislativos, como el surgimiento de nuevos derechos. También se hablará del régimen sancionador de la protección de datos, viendo las consecuencias que puede conllevar el incorrecto tratamiento de datos. Además, se verán los derechos digitales de la legislación vigente, en el ámbito laboral. Finalmente se verá la Agencia Española de Protección de Datos.

1 Evolución de la protección de datos

El derecho fundamental a la protección de datos en España deriva de lo establecido en el artículo 18.4 de la Constitución Española, *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos",* no obstante, hay que tener en cuenta que la Constitución fue promulgada en 1978, momento en el que el desarrollo de las tecnologías informáticas y de Internet, no era previsible. Pese a esto, se aceptó una enmienda que tuvo como resultado este último inciso, el cual con el tiempo ha demostrado ser idóneo para la protección frente al uso de la informática. No obstante, hay que tener en cuenta que esa protección ha de ser desarrollada por una ley.

Y es que, *"El derecho a la protección de datos personales tiene, en su configuración constitucional, un marcado carácter instrumental. Se encuentra al servicio de otros derechos. Concretamente, garantiza el honor y, la intimidad personal y familiar de los ciudadanos y, el pleno ejercicio de sus derechos. Por lo tanto, amplía el ámbito de protección de estos derechos, preservándolos frente al uso de las nuevas tecnologías."* (Orellana Cano, 2019, pág. 32 y 33)

Como se ha visto, la Constitución establece en el artículo 18.4, que la ley limitará el uso de la informática. Para dar cumplimiento a este mandato entró en vigor en el año 1992 la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. En la Exposición de Motivos, el legislador habla de la privacidad y cómo las nuevas tecnologías informáticas la han expuesto a nuevos peligros, así mismo, diferencia entre intimidad y privacidad. En palabras del legislador *"la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona"*, también considera que está suficientemente protegida por los tres primeros párrafos del artículo 18 de la Constitución y sus leyes de desarrollo. En cuanto a la privacidad el legislador dice que *"constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado"*, además dice que

hasta ese momento estaba protegida por el tiempo y el espacio, sin embargo con las nuevas tecnologías informáticas esto ha desaparecido.

En el 14 de enero de 2000 esta Ley fue derogada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el objeto de esta Ley es garantizar y proteger los derechos fundamentales y libertades públicas, en especial los derechos al honor y a la intimidad personal y familiar, en el tratamiento de los datos personales. Esta ley muestra que la protección de datos tiene carácter instrumental. Esta norma fue derogada en 2018 por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, la cual se encuentra vigente, esta norma viene a adaptar la legislación española a la nueva normativa europea en esta materia, en especial al RGPD, del que se habló anteriormente.

2 Ley Orgánica 3/2018

La Ley Orgánica 3/2018 aborda los nuevos desafíos en protección de datos que se han dado por la evolución tecnológica. Es indudable el rápido avance tecnológico que se ha vivido desde los años 90 hasta la actualidad, lo que ha conllevado un cambio en las relaciones sociales, incluidas las relaciones laborales. Pese a que las nuevas tecnologías presentan numerosos beneficios, como el poder comunicarse y transmitir archivos a distancia de forma inmediata, también presenta nuevos riesgos, especialmente para la intimidad de las personas. Para proteger a las personas de estos riesgos la nueva ley recoge en su Título X los derechos digitales y los derechos aplicables a Internet, entre estos derechos se encuentran algunos del ámbito laboral que se analizarán más adelante. Entre los artículos 13 y 18, la ley establece una serie de derechos que pueden ejercitar los interesados, estos derechos son:

- Derecho de acceso. Este derecho establece que los interesados pueden obtener la información sobre el tratamiento de sus datos de carácter personal.
- Derecho de rectificación. Este derecho consiste en la posibilidad de que el interesado pueda completar un dato incompleto o corregir un dato erróneo.
- Derecho de supresión (derecho al olvido). Este derecho otorga al interesado la posibilidad de suprimir sus datos personales facilitados.
- Derecho a la limitación del tratamiento. Este derecho otorga al interesado la posibilidad, siempre que se cumplan unas circunstancias concretas, de limitar sus datos personales. Durante esta limitación, para cualquier tratamiento se deberá contar con la autorización del interesado, excepto cuando sea por razones de interés público importante, para proteger los derechos de otra persona o para reclamaciones.
- Derecho a la portabilidad de los datos. Este derecho consiste en que el interesado puede transferir sus datos personales de un responsable del tratamiento a otro.

- Derecho de oposición. Este derecho habilita la posibilidad de que el interesado se oponga en cualquier momento al tratamiento de sus datos personales.
- Derecho a no ser objeto de una decisión individual basada únicamente en el tratamiento automatizado. Y es que, *"Este derecho ha de tenerse en cuenta, en el ámbito laboral, en relación con la elaboración de las listas negras."* (Orellana Cano, 2019, pág. 92)

Los actores involucrados en la protección de datos son: el interesado, el responsable del tratamiento, el encargado del tratamiento y el delegado de protección de datos.

El interesado es la persona física de la cual se recaban los datos personales, así mismo es la persona cuyos derechos pretende proteger la ley.

El responsable del tratamiento es la persona física o jurídica responsable del tratamiento de los datos personales, así como de la garantía de los derechos de los afectados. Deberá determinar las medidas de seguridad apropiadas para que el tratamiento sea realizado conforme a la legalidad.

El encargado del tratamiento puede ser una persona física o jurídica, una autoridad pública, un servicio o un organismo designado por el responsable del tratamiento. El encargado presta un servicio al responsable del tratamiento que conlleva el tratamiento de datos personales, deberá de seguir las instrucciones dadas por el responsable, no podrá usar los datos para una finalidad diferente a la que el responsable le indicó en el momento que se facilitaron. El encargado y el responsable deberán de formalizar un contrato en el que se establezca el objeto, duración, naturaleza y la finalidad del tratamiento.

El delegado de protección de datos será designado por el responsable y el encargado del tratamiento de datos, cuando sea obligatorio o de forma voluntaria cuando no lo sea. El delegado, que puede ser una persona física o jurídica, debe de ser nombrado teniendo en cuenta sus cualificaciones profesionales, su conocimiento legislativo y la práctica en materia de protección de datos. El delegado tendrá total autonomía y le tendrá que facilitar el responsable o el encargado todos los recursos necesarios para desarrollar su actividad, incluidos el acceso a los datos personales y procesos de tratamiento. El responsable y el encargado deberán de comunicar en un plazo de 10 días los nombramientos y ceses de los delegados a la Agencia Española de Protección de Datos (AEPD) o a la autoridad autonómica competente. Tanto la AEPD como la autoridad autonómica deberán mantener una lista actualizada de delegados, la cual deberá de ser accesible por medios electrónicos.

Las organizaciones tienen unas obligaciones en el tratamiento de datos, entre estas se encuentra la obligación de tener el consentimiento del afectado por el tratamiento de datos. También está obligada a notificar acerca de una violación de seguridad, si esta afecta a datos personales y constituye un riesgo para los derechos y las libertades del afectado. Otra obligación es la de informar al afectado por el tratamiento del nombre del responsable, la razón por la que podemos tratar sus datos (legitimación), para que van a ser

usados sus datos y cómo puede ejercitar sus derechos. El responsable y el encargado del tratamiento de datos deben llevar un registro de actividades de tratamiento, en el que se indique la siguiente información:

- Nombre y datos de contacto del responsable y del delegado de protección de datos.
- Fines del tratamiento.
- Descripción de las categorías de interesados.
- Descripción de las categorías de datos personales.
- Categorías de destinatarios a los cuales se comunicarán los datos personales.
- La documentación de garantías adecuadas cuando se trasfieran datos personales a un tercer país o una organización internacional.
- Si es posible, los plazos de supresión de los datos según su categoría y una descripción general de las medidas de seguridad.

Como ya se indicó otra obligación es nombrar un delegado de protección de datos en algunos supuestos como, por ejemplo, cuando se trate de: colegios profesionales, centros docentes o entidades que traten de forma habitual y sistemática datos personales a gran escala. Las organizaciones también tienen la obligación de realizar una Evaluación de Impacto relativa a la Protección de Datos con la finalidad de describir de forma anticipada y preventiva, un tratamiento de datos personales, así mismo se evalúa su necesidad y proporcionalidad y las medidas necesarias para reducir los potenciales riesgos que se hayan detectado.

Los responsables y encargados del tratamiento deberán realizar un análisis de riesgos de la seguridad de la información con la finalidad de establecer las medidas de seguridad y control que permitan garantizar los derechos y libertades de las personas.

Los principios del tratamiento de los datos personales no vienen recogidos en la esta ley, sin embargo, como se verá en el régimen sancionador, la vulneración de estos durante el tratamiento puede suponer una infracción muy grave. Los principios se encuentran recogidos en el artículo 5 del RGPD y son:

- Principio de licitud, transparencia y lealtad. Los datos serán tratados de forma lícita, leal y transparente para el interesado.
- Principio de limitación de la finalidad. Los datos serán recogidos y tratados con fines determinados, explícitos y legítimos.
- Principio de minimización de datos. Los datos serán adecuados, pertinentes y limitados a la finalidad para la que son tratados.
- Principio de exactitud. Los datos son exactos, en el caso de no serlo serán actualizados o suprimidos.
- Principio de limitación del plazo de conservación. Los datos se mantendrán el plazo necesario para cumplir la finalidad por la que son tratados.

- Principio de integridad y confidencialidad. Los datos serán tratados con las medidas de seguridad adecuadas, las cuales deberán de protegerlos del tratamiento no autorizado, su pérdida o cualquier otra amenaza.
- Principio de responsabilidad proactiva. Los responsables del tratamiento deberán de aplicar las medidas adecuadas para garantizar el tratamiento de datos respetando el RGPD, así mismo deberán de poder demostrarlo.

3 Régimen sancionador en la Ley Orgánica 3/2018

El régimen sancionador para las infracciones en materia de protección de datos se encuentra en el Título IX de la Ley Orgánica 3/2018, la cual remite gran cantidad de veces al RGPD como se verá a continuación.

Las infracciones pueden ser de tres tipos atendiendo a su gravedad: muy graves, graves y leves. En cuanto a quienes estarán sujetos a este régimen la ley establece que serán: los responsables y encargados de los tratamientos, las entidades de certificación, las entidades acreditadas de supervisión de los códigos de conducta y los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.

A la hora de tipificar las situaciones que serán consideradas muy graves, graves o leves, se ve que están en función de lo que dice el RGPD, si bien la ley es mucho más específica y clara a la hora de decir que situaciones constituyen infracciones y sanciones, también especifica los plazos de prescripción.

A continuación, se va a nombrar algunas de las situaciones que se consideran infracciones muy graves, graves y leves, así como cuáles son sus plazos de prescripción:

- Las infracciones muy graves tienen un plazo de prescripción de 3 años. Las situaciones son principalmente las que suponen una vulneración sustancial del tratamiento que tenga que ver con el uso de los datos para una finalidad que es incompatible con la que fueron recogidos, la omisión del deber de informar sobre el tratamiento, la vulneración del deber de confidencialidad, la exigencia del pago al afectado para facilitarle información o atender su solicitud de ejercicio de derechos, el tratamiento de datos vulnerando los principios de tratamiento, entre otros.
- Las infracciones graves tienen un plazo de prescripción de 2 años. Las situaciones son principalmente la vulneración sustancial del tratamiento de datos personales de un menor cuando no se recaba su consentimiento, o el del titular de la patria potestad, cuando no se acredita la realización de los esfuerzos razonables a la hora de verificar la validez del consentimiento prestado por un menor, la falta de medidas técnicas y organizativas apropiadas para aplicar el principio de protección de datos desde el diseño, entre otros.

- Las infracciones leves tienen un plazo de prescripción de 1 año. Las situaciones son, por ejemplo, la exigencia de pagar un canon por facilitar información obligatoria al afectado o incumplir el principio de transparencia de la información o el derecho de información del afectado, al no facilitar la información dispuesta en los artículos 13 y 14 del RGPD. El artículo 13 establece la información que deberá facilitarse cuando los datos personales se obtengan del interesado y el artículo 14 cuando no se hayan obtenido del interesado.

En cuanto a la prescripción de las infracciones se debe tener en cuenta que esta se interrumpirá cuando se inicie el procedimiento sancionador y el interesado lo conozca, así mismo si el expediente sancionador estuviera paralizado durante más de seis meses, por causa no imputable al presunto infractor, volverá a trascurrir el plazo de prescripción.

La cuantía de las sanciones administrativas dependerá de la infracción, para determinar la cuantía la Ley nos remite al RGPD, el cual establece dos cuantías máximas dependiendo de la gravedad. Las más graves serán sancionadas hasta 20 millones de euros o el 4% del volumen de facturación anual de la empresa. Las menos graves serán sancionadas con hasta 10 millones de euros o el 2% del volumen de facturación anual de la empresa. Para determinar las cuantías se deberá de tener en cuenta los dispuesto en el artículo 83.2 del RGPD, el cual indica que para determinar la cuantía se debe de tener en cuenta la naturaleza, gravedad, duración, intencionalidad, las medidas tomadas para paliar los daños, el grado de responsabilidad, la cooperación, entre otras. La AEPD será la encargada de imponer las sanciones y determinar la cuantía.

Por otra parte, el afectado por una infracción podrá tener derecho a una indemnización por parte del responsable o el encargado del tratamiento, con la finalidad de resarcir los daños y perjuicios sufridos. (Instituto Nacional de Ciberseguridad, 2018)

Se debe agregar que algunas infracciones en materia de protección de datos pueden tener consecuencias penales. Es el caso del ciberacoso, por ejemplo, el cual se encuentra recogido en el Código Penal y puede conllevar penas de prisión.

4 Derechos digitales en el ámbito laboral en la Ley Orgánica 3/2018

Como se ha indicado previamente, el Título X de la Ley Orgánica 3/2018 recoge los derechos digitales y los derechos aplicables a Internet, entre los cuales se encuentran alguno específicos del ámbito laboral.

Estos derechos del ámbito laboral son los establecidos en los artículos 87, 88, 89, 90 y 91, a continuación, se va a explicar brevemente en que consiste cada uno.

El artículo 87 establece el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral, el cual deriva directamente del artículo 18 de la Constitución que se vio previamente.

Este derecho, que se da cuando el empleador pone a disposición del empleado dispositivos digitales, pretende que los empleados tengan protegida su intimidad cuando los usen. Esto no quiere decir que se

pueda usar estos dispositivos como si fueran de su propiedad, ya que el empleador podrá acceder al dispositivo a los solos efectos de garantizar la integridad de estos y controlar el cumplimiento de las obligaciones laborales o estatutarias. Pero se puede dar el caso de que el empleador haya autorizado el uso con fines privados de los dispositivos, cuando se dé esto el empleador podrá acceder al contenido del dispositivo siempre que haya especificado de modo preciso los usos autorizados y haya establecido garantías que preserven la intimidad de los trabajadores. Además, los empleadores deben de establecer, con la participación de los representantes legales de los trabajadores, los criterios de utilización de los dispositivos respetando en todo caso la protección a la intimidad del trabajador, de acuerdo con los derechos constitucionales y legales, así como con los usos sociales.

El artículo 88 establece el derecho a la desconexión digital en el ámbito laboral, la principal finalidad de este derecho es evitar que los trabajadores continúen trabajando fuera de su jornada laboral. Este derecho cobra mayor importancia con forme avanza la tecnología, ya que cada vez más trabajadores pueden trabajar sin necesidad de acudir físicamente a la empresa, esto puede ocasionar que los trabajadores alarguen su horario laboral. Este alargamiento se puede dar por el establecimiento de fechas límite en las empresas, para terminar determinados trabajos, por ejemplo. Por otro lado, este alargamiento puede tener efectos negativos sobre su salud, produciendo estrés y tensión, además de influir en su tiempo de descanso, su intimidad y su conciliación de la vida personal y familiar con la actividad laboral. Para proteger este derecho la ley establece que el empleador deberá elaborar una política interna dirigida a los trabajadores, en la que definirá las modalidades de ejercicio de este derecho, así como las acciones formativas y de sensibilización del personal para evitar la fatiga informática producida por el uso de las herramientas tecnológicas.

El siguiente derecho, artículo 89, se refiere al derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. El uso de algunos de estos dispositivos es habitual en algunas empresas, por las características de estas, como podría ser establecimientos de venta o sucursales bancarias. En estos lugares su principal propósito no es vigilar a los trabajadores, es evitar que se produzcan robos. Pese a esto el empleador tiene la potestad, tal como indica el artículo 20 del Estatuto de los trabajadores, de vigilar y controlar con la finalidad de comprobar que los trabajadores cumplen con sus obligaciones y deberes laborales. Para llevar a cabo esta potestad el empleador puede hacer uso de dispositivos de videovigilancia, pero de forma previa deberá de informar de forma expresa, clara y concisa, tanto a los trabajadores como a sus representantes del uso de estos dispositivos. No obstante, si se capta la comisión flagrante de un acto ilícito por parte de los trabajadores, el deber de informar se entenderá cumplido cuando hubiera al menos un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos entre los artículos 13 y 18 de la Ley 3/2018 (mismo derechos que los previstos en los artículos 15 a

22 del RGPD), los cuales vimos anteriormente. En cuanto al uso de sistemas de grabación de sonidos en el lugar de trabajo solo será posible cuando debido a la actividad que se desarrolle en el centro de trabajo, se den riesgos relevantes para la seguridad de las personas, instalaciones y bienes, y respetando los principios de proporcionalidad y de intervención mínima.

Lógicamente la instalación de cualquiera de estos dispositivos no está permitida en ninguna circunstancia en los lugares que los trabajadores tienen destinados a su descanso o esparcimiento, como vestuarios, comedores, aseos u otros con similar finalidad, ya que supondría una vulneración de su intimidad.

El próximo derecho, artículo 90, es el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral. Este derecho guarda grandes similitudes con el anterior derecho ya que, al igual que este surge para limitar la potestad de vigilancia y control del empleador, el cual puede tratar los datos que obtenga de los sistemas de geolocalización para ejercer funciones de control de los trabajadores. Estos sistemas de geolocalización tiene sentido usarlos cuando se trata de trabajadores con puestos de trabajo fuera de las instalaciones de la empresa o cuando estas son muy extensas, por ejemplo, se pueden usar en transportistas o agentes comerciales. Al igual que el anterior derecho, antes de usar estos sistemas el empleador deberá de informar de la existencia y características de estos, de forma expresa, clara e inequívoca, tanto a los trabajadores como a sus representantes, y también deberá de informarles sobre el posible ejercicio de los derechos previstos entre los artículos 13 y 18 de la Ley 3/2018.

Para terminar estos derechos, el artículo 91, no establece un derecho propiamente dicho, sino que otorga a la negociación colectiva una especial relevancia. Este artículo establece que los derechos digitales no podrán ser restringidos mediante la negociación colectiva, pero sí que podrán ser mejorados, estableciendo garantías adicionales en los convenios colectivos. Esto supone que, se pueda desarrollar estos derechos, adaptándolos a las características de cada sector, ya que lo que para un sector puede ser un derecho que haya que desarrollar por el alto uso de ciertos dispositivos, en otros puede ser que no sea necesario por no usar esos dispositivos. Y es que, *"En ocasiones, las reglas generales no podrán ofrecer, en mi opinión, las soluciones a muchos de los problemas específicos de la protección de datos personales en el desarrollo de la actividad laboral, lo que, sin embargo, se podrá conseguir mediante la negociación colectiva, que contemplará la diversidad de situaciones y el régimen específico para hacer frente a las mismas desde el respeto a este derecho fundamental y, la transparencia en el tratamiento de los datos personales."* (Orellana Cano, 2019, pág. 71)

5 La Agencia Española de Protección de Datos

La AEPD es una autoridad administrativa independiente de ámbito estatal que viene reconocida en el Título VII de la Ley 3/2018. Cuenta con personalidad jurídica propia y plena capacidad pública y privada, además actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Sus principales funciones son:

- Controlar la aplicación de la normativa en materia de protección de datos.
- Promover la sensibilización del público y la compresión de los riesgos, normas, garantías y derechos en materia de protección de datos.
- Asesoramiento del Parlamento, el Gobierno, así como otras instituciones y organismos, en materia de protección de datos.
- Sensibilizar a los encargados y responsables del tratamiento sobre las obligaciones que tienen en virtud del RGPD.
- Facilitar información a cualquier interesado sobre el ejercicio de sus derechos en materia de protección de datos.

La AEPD tiene tres tipos de poderes:

- De investigación. Como ordenar a los responsables o encargados del tratamiento que faciliten cualquier información que necesite para realizar sus funciones. O como llevar a cabo investigaciones mediante auditorias de protección de datos.
- Correctivos. Como sancionar las infracciones en materia de protección de datos, pudiendo imponer multas administrativas.
- De autorización y consultivos. Como asesorar al responsable del tratamiento o emitir dictámenes y aprobar proyectos de códigos de conducta.

También es la encargada de representar a España en los foros internacionales de protección de datos.

La página web de la AEPD, www.aepd.es, cuenta con herramientas y guías, así como con información sobre protección de datos. Entre las herramientas se encuentran algunas cuya finalidad es atender consultas de los encargados y responsables del tratamiento, así como del delegado de protección de datos. La AEPD cuenta en la web con gran cantidad de guías, las cuales van desde el uso de las cookies hasta guías del RGPD para responsables del tratamiento. Además, la web dispone de un apartado en el cual cualquier persona interesada puede conocer sus derechos y deberes en materia de protección de datos.

Cuando se publicó la Ley 3/2018, la AEPD elaboró y publicó en su web un documento sobre las novedades que presentaba la nueva ley (Agencia Española de Protección de Datos, 2019). Este documento tiene la finalidad de informar de forma general de las novedades, como la obligación de informar a los ciudadanos sobre el tratamiento de sus datos y el ejercicio de sus derechos.

IV. Protección de datos en el Departamento de Recursos Humanos

Dada la naturaleza del departamento de Recursos Humanos, la protección de datos es un tema de vital importancia. Hay que tener en cuenta que se tratan gran cantidad de datos personales de los trabajadores, al igual que con personas ajenas a la empresa como, por ejemplo, candidatos que envían su *curriculum vitae*. Todos estos datos personales deben de ser tratados respetando lo dispuesto legalmente, así como con seguridad y confidencialidad. Otra función que generalmente tiene el departamento de Recursos Humanos es el control de la asistencia al trabajo. Este control suele realizarse mediante dispositivos digitales y, por tanto, la gestión de sus datos cobra vital relevancia. Es importante que los empleados del departamento conozcan los requisitos de su uso.

Aunque muchos aspectos de la protección de datos son comunes para los diferentes departamentos de una empresa, hay otros que son específicos del departamento de Recursos Humanos, como se ha visto anteriormente en la Ley 3/2018. Pese a esto, la protección de datos debe ser un único sistema dentro de la empresa, en el que cada departamento realice la protección de datos de la misma forma, pero teniendo en cuanta las posibles especificidades que pudieran tener, como en el caso de Recursos Humanos.

En cuanto a la protección de datos personales en el ámbito laboral se puede diferenciar tres momentos: el primero sería en el acceso al trabajo, el segundo sería durante la vigencia del contrato y el tercero sería en la extinción del contrato.

A continuación, se van a tratar las diferentes normas internacionales de la *International Organization for Standardization* (ISO)[2]. Estas normas no tienen carácter obligatorio para las empresas, si bien aplicarlas y certificarlas puede aportar beneficios, tanto en seguridad como en economía, ya que puede suponer una ventaja competitiva.

Después de las normas ISO se tratará la política de seguridad y tratamiento de datos que tiene que llevar a cabo el departamento de Recursos Humanos. Dentro del marco de dicha política, se explicarán cuáles son las medidas de seguridad que pueden llevarse a cabo durante el tratamiento, la clasificación de los datos y como debe de actuar el personal durante los tres momentos nombrados anteriormente.

1 Normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27701

La ISO/IEC 27001 (International Organization for Standardization, 2013) es una norma internacional que especifica como se debe de implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) en cualquier tipo de organización, con independencia de su titularidad, tamaño o fin.

[2] Organización internacional formada por organizaciones nacionales de normalización, cuya finalidad es crear estándares internacionales voluntarios. La Asociación Española de Normalización (UNE) es miembro de la ISO.

Para la ISO/IEC 27001 la gestión de la seguridad de la información no se limita a las tecnologías de la información (TI), sino que se extiende a todos los ámbitos, tratando también la protección física, la protección jurídica o la seguridad en el departamento de recursos humanos entre otros.

La ISO/IEC 27001 busca la gestión de riesgos, mediante la investigación con el propósito de saber dónde se encuentran, para posteriormente tratarlos con las medidas que sea necesario. Las medidas contempladas en la norma son de diverso tipo, pueden ser de carácter técnico, como software, hardware u otros equipos dependiendo del riesgo, también pueden ser políticas o procedimientos.

La ISO/IEC 27002 (International Organization for Standardization, 2013), a diferencia de la ISO/IEC 27001, no es certificable y establece solo recomendaciones y buenas prácticas. Esta norma complementa la información de los anexos de la ISO/IEC 27001, los cuales describen los mecanismos y dominios de control. La ISO/IEC 27002 cuenta con 14 capítulos y 114 controles recomendados, si bien no es necesario cumplirlos todos para obtener la certificación de la ISO/IEC 27001, ya que dependerá de la estrategia de riesgo y el tipo de empresa. Uno de los capítulos trata la seguridad relativa a los recursos humanos, esta seguridad es muy importante ya que la mayoría de los incidentes de seguridad que ocurren en las organizaciones tiene su origen en un error humano. Por eso es muy importante que los trabajadores estén formados y concienciados de cómo deben emplear la información en su puesto de trabajo, así como de la importancia de un nivel de seguridad acorde a los datos e información manejada.

En la gestión de los Recursos Humanos la norma habla de 3 momentos diferentes del trabajador en su relación con la empresa: antes de la contratación, durante el empleo y cuando termina su relación laboral o cambia de puesto. Para cada uno de estos momentos la norma habla de diferentes aspectos que deberán de realizarse.

Antes de la contratación se deberá de investigar los antecedentes del candidato, dentro de los límites legales, respetando las leyes normas y códigos éticos. También se deberán de establecer en el contrato de trabajo los términos y condiciones de la relación laboral en materia de seguridad de la información.

Durante el empleo se deberá establecer responsabilidades en la gestión, exigiendo a los empleados y contratistas que cumplan con las medidas del sistema de seguridad de la información. Los empleados y contratistas deberán de recibir la formación, capacitación y concienciación adecuados para su puesto de trabajo en la organización. Deberá de existir un proceso disciplinario formal, comunicado a los empleados previamente, que detalle las acciones que se deberán de tomar con los empleados que cometan una violación de la seguridad de la información.

Cuando termina la relación contractual o cambia de puesto, hay que definir las responsabilidades y obligaciones de seguridad de la información que continuarán vigentes cuando finalice la relación contractual o se cambie de puesto, estas deberán de ser comunicadas y se deberán de cumplir.

La ISO/IEC 2770 (International Organization for Standardization, 2019) es una extensión certificable de la ISO/IEC27001, por lo que para obtenerla deberá de tener la certificación de la ISO/IEC27001. Su objetivo es la mejora del Sistema de Gestión de Seguridad de la Información en materia de privacidad, para ello establece los requisitos para establecerlo, implementarlo, mantenerlo y mejorarlo continuamente. Esta norma es la más reciente, siendo su publicación en el año 2019. Además, incluye en su Anexo D un mapeo de los controles al nuevo RGPD, el cual se aplica en la Unión Europea desde el 25 de mayo de 2018.

Estas normas se basan en la mejora continua, para ello aplican el ciclo de Deming o ciclo PDCA, *Plan-Do-Check-Act* o en español Planificar-Hacer-Verificar-Actuar. El ciclo PDCA busca la mejora continua para ello cuenta con 4 pasos cíclicos que se deben de realizar en orden.

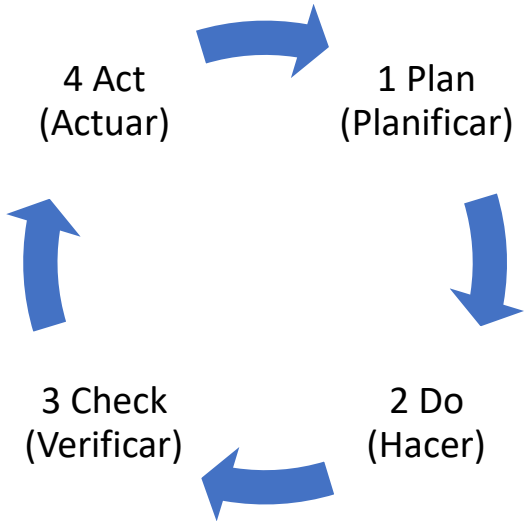

Figura 1 Ciclo de Deming o PDCA

El primer paso es el de *Plan* (Planificación) en el cual se busca las actividades que deben de mejorar y se marca el objetivo de la mejora. En este paso se pueden usar herramientas que ayuden a la planificación como el Diagrama de Gantt, el cual consiste en exponer gráficamente el tiempo de dedicación previsto para las diferentes actividades.

El segundo paso es el de *Do* (Hacer) en el cual se realizan los cambios que son necesarios para implantar la mejora continua.

El tercer paso es el de *Check* (Verificar) en el cual se evalúa en que grado se ha conseguido la mejora, para ello ha debido de pasar un tiempo, tras el cual se recopilan los datos de control para ser analizados. En este paso se pueden usar herramientas de evaluación tales como el Diagrama de Pareto, que consiste en organizar gráficamente los datos en función de su importancia, permitiendo establecer un orden de prioridades.

El cuarto paso es el de *Act* (Actuar) en el cual a partir de los datos obtenidos en el paso anterior se implanta de manera definitiva la mejora en caso de que la evaluación fuera satisfactoria, y en caso de no

serlo se decidiría si hay que hacer cambios o hay que desecharla. En este paso se pueden usar herramientas de mejora continua como el Método de Kaizen, el cual busca la mejora continua en todos los aspectos de la organización, implicando a todos los integrantes de esta. Para que el método funcione se deben de respetar los valores sobre los que se asienta: compromiso, disciplina y constancia.

La certificación de la ISO/IEC 27701 y de la ISO/IEC 27001 tiene que ser llevada a cabo por una empresa externa, independiente y acreditada, la cual auditará el grado de implantación y de eficacia de las normas y, en el supuesto de que la auditoria de un resultado positivo, emitirá la correspondiente certificación.

Obtener estas certificaciones aporta beneficios a la empresa, ya que es una manera de demostrar de forma independiente el cumplimiento del RGPD, así como de las leyes y normativas en materia de seguridad de la información. Además, se puede obtener una ventaja competitiva, dado que se demuestra a los clientes que la seguridad de la información, incluida la suya, es de vital importancia para la empresa. Otro beneficio es que los trabajadores de la empresa ven que su información se encuentra protegida, que los riesgos están identificados, han sido evaluados y tratados, lo que les produce seguridad. Además, hace que la empresa sea más codiciada cuando publica ofertas de trabajo.

2 Política de Seguridad y Tratamiento de Datos en el Departamento de Recursos Humanos

Es muy importante que los integrantes del departamento de recursos humanos sepan cómo deben de tratar los datos personales y los datos sensibles para la organización. Para ello es necesario que la empresa previamente disponga de una política general de seguridad y tratamiento de datos. Cada departamento de la empresa puede tener, por sus propias características, especificidades en la seguridad y tratamiento de los datos, por lo que es recomendable que la empresa disponga de políticas concretas para cada departamento, o que estas sean incluidas en la política general.

Centrándonos en el departamento de Recursos Humanos, es obvio que los integrantes manejan información personal de los trabajadores e incluso de personas que son ajenas a la organización, esto ocasiona que en el departamento se deba de tener especial cuidado con la información. Por ejemplo, no se debe de dejar un *curriculum vitae* en una bandeja archivadora de forma permanente, salvo que se encuentre en un lugar al que solo pueden acceder los encargados de su tratamiento, en este caso los integrantes del departamento de Recursos Humanos. Esto se debe a que, si el documento se encuentra en un lugar de fácil acceso, puede darse el caso de que alguien lo sustrajerá o copiará, obteniendo datos personales. Este hecho podría derivar en consecuencias legales para la empresa.

Además, también hay que tener en cuenta los nuevos riesgos derivados del uso de tecnologías en la empresa, ya que en la actualidad los riesgos pueden ser tanto físicos, como digitales. Esto hace que los integrantes del departamento de Recursos Humanos deban de ser debidamente formados en ciberseguridad.

A continuación, se va a tratar como debe actuar el personal de recursos humanos en tres momentos diferentes que se dan durante una relación laboral: el momento de acceso al trabajo, el momento de vigencia del contrato y el momento de extinción del contrato. Posteriormente se tratará la clasificación de los datos y la seguridad durante su tratamiento en el departamento de Recursos Humanos, tomando como referencia las diferentes políticas de seguridad del Instituto Nacional de Ciberseguridad (INCIBE).

A. Cómo debe actuar el personal de Recursos Humanos

Desde el departamento de Recursos Humanos se debe de actuar teniendo en cuanta la importancia de los datos que se usan y las consecuencias que puede tener un mal uso, para la empresa y para el trabajador del departamento que los usa.

El personal del departamento deberá de conocer lo que establecen el RGPD y la Ley Orgánica 3/2018, en el ámbito laboral, ya que se establecen nuevos derechos laborales para los trabajadores.

El personal del departamento deberá de conocer también que medidas de seguridad debe de tomar cuando se manejen datos, los cuales deberán de ser clasificados previamente, para saber cuáles son las medidas de seguridad y como se debe de usarlos.

Una de las principales actuaciones que deben realizar en el departamento es informar a los trabajadores sobre sus derechos, deberes y responsabilidades sobre la seguridad de la información, explicándoles las sanciones y consecuencias que puede conllevar un acto negligente.

En el departamento de recursos humanos hay tres momentos diferentes en los que las actuaciones que se tienen que llevar a cabo son totalmente diferentes.

El primer momento es el de acceso al trabajo de nuevos trabajadores y el proceso previo que esto conlleva. En este momento el interesado no es necesario que dé su consentimiento de forma expresa, ya que el RGPD dice que el tratamiento será licito cuando sea necesario para la ejecución de contratos y precontratos en los que el interesado sea parte. Durante los procesos de selección la información es facilitada por el interesado, pero además de esa información desde la empresa se consigue más información por otros medios.

Durante los procesos de selección lo habitual es que los interesados hagan llegar a la empresa su *curriculum vitae,* una vez en la empresa, este documento debe de contar con la protección debida, ya que se trata de datos personales, aunque la empresa se limite únicamente a conservarlo. La empresa deberá de cumplir con el deber de información, la forma de cumplirlo será dependiendo del medio por el que llegue el *curriculum vitae.* Por ejemplo, si el interesado lo presenta en la empresa se le podrá informar en ese momento usando un medio que deje constancia o en el caso de que sea remitido por correo electrónico o postal, se le podrá remitir la información utilizando el mismo medio.

En relación a la conservación hay que tener en cuenta, como indica Preciado Domènech (2017), que la determinación del periodo de conservación se usa doctrinalmente las pautas que contiene la Recomendación CM/Rec(2015)5, del Comité de Ministros del Consejo de Europa, de 1 de abril de 2015. Esto significa que solo podrán ser conservados durante el tiempo necesario para cumplir la finalidad perseguida, por lo que en caso de que antes de finalizar el periodo de selección, se supiera que un candidato no va a ser contratado, se debería de borrar de forma segura los datos personales o deberán de ser retirados por el interesado. No obstante, se podrán conservar para futuros procesos de selección, si se ha informado debidamente de esto al interesado, comunicándole que puede ejercer el derecho de cancelación del que se habló con anterioridad.

Con las nuevas tecnologías se ha posibilitado al empleador obtener datos personales de los candidatos fácilmente, sin que estos los faciliten. Esto se debe a que en Internet se acumula gran cantidad de información personal, por ejemplo, en redes sociales como Facebook, Twitter o Instagram. Al igual que la información que nos facilita el candidato, no será necesario el consentimiento explícito, cuando los datos sean necesarios para la ejecución de contratos y precontratos en los que el interesado sea parte, sin embargo, sí que tendrá que cumplir el deber de información. El hecho de que los datos se encuentren públicamente accesibles no quiere decir que el empleador pueda tratarlos ilimitadamente, sino que, *"Deberá tener en cuenta el límite de la finalidad, es decir, en su caso, el tratamiento se deberá de realizar de acuerdo con fines concretos."* (Orellana Cano, 2019, pág. 115)

El segundo momento es la vigencia de la relación laboral. Durante este periodo los integrantes del departamento de recursos humanos deben de controlar la prestación de servicios del trabajador, además deben de elaborar las nóminas. Durante la elaboración de las nóminas de los trabajadores se tratan datos personales de los trabajadores, debido a esto los encargados de realizarlas deberán de tomar las medidas de seguridad adecuadas. Como se verá posteriormente, hay que tener en cuenta que las únicas personas que deben de tener acceso a las nóminas son el trabajador al que corresponde la nómina y el encargado de realizarla. En este momento también se tratan datos sobre sanciones, estos datos deberán de ser destruidos o cancelados, en virtud del derecho de cancelación que posee el interesado, cuando el plazo de prescripción este cumplido.

En cuanto a los datos obtenido del control de la prestación de servicios, ya vimos anteriormente dos supuestos que gozan de especial relevancia. Estos son el uso de dispositivos de videovigilancia y grabación de sonidos, así como los sistemas de geolocalización, en los artículos 89 y 90 de la Ley 3/2018 encontramos como se aplica el derecho a la intimidad frente al uso de estos dispositivos. Además de estos medios de control, hay otros como el uso de tarjetas de identificación en un lugar visible mientras trabajan en la empresa, estas tarjetas podrán incluir la fotografía del trabajador y su número de D.N.I. Otro método es el uso de sistemas biométricos. Si se usa este último método no se necesita el consentimiento del trabajador, ya que se considera que es necesario para la formalización del contrato, por otro lado, el deber de

información será cumplido al tomar la huella al trabajador, ya que en ese momento se indicará al trabajador para que se hace eso.

El tercer y último momento es el de la extinción de la relación laboral. En este momento surge la necesidad de que hacer con los datos que se tienen. Ya hemos visto el caso de los *curriculums vitae* y las sanciones que recibió el trabajador, pero no podemos pasar por alto que algunas sanciones pueden conllevar la sanción máxima dentro de la empresa, el despido. En estos casos es habitual que el trabajador lo impugne judicialmente. La empresa, para demostrar que el despido es lícito, aportará al procedimiento las debidas pruebas, siendo por ejemplo obtenidas mediante videovigilancia o mediante sistemas de geolocalización. Es muy importante que la prueba se haya obtenido lícitamente, ya que, de no ser así, la empresa habrá vulnerado un derecho fundamental, lo que supone que el despido sea nulo. Esta nulidad conlleva que el trabajador deberá ser readmitido de inmediato. Además se le deberán de abonar los salarios que dejo de percibir desde el momento que fue despedido hasta la reincorporación, si bien existen dos supuestos que lo modifican: si el trabajador encontró otro trabajo se podrá descontar los salarios que percibió en el nuevo trabajo, y si ha percibido prestaciones por desempleo, en cuyo caso la empresa le ingresará a la Seguridad Social las cantidad que percibió el trabajador por la prestación, el trabajador además deberá de percibir por parte de la empresa la diferencia que queda entre lo que cobro de la prestación y el salario.

B. Clasificación de los datos en el departamento

Para garantizar la seguridad de la información debe de ser clasificada, según el Instituto Nacional de Ciberseguridad, los activos de información deben de ser clasificados atendiendo a los criterios de confidencialidad, disponibilidad e integridad, teniendo en cuenta el impacto que tendría su pérdida, destrucción, difusión, acceso no autorizado o alteración. (Instituto Nacional de Ciberseguridad)

Para realizar esta clasificación se debe de realizar un inventario de la información, indicando si se puede, su tamaño, ubicación, personas responsables, quien tiene acceso, así como cualquier otro dato que consideremos útil para la clasificación.

Si clasificamos la información en base a su confidencialidad, tendremos cuatro niveles:

- Información pública: Esta información es accesible para todo el mundo de forma pública, como podría ser un informe de sostenibilidad o una memoria anual.
- Información interna: Esta información solo es accesible para el personal de la empresa, como podría ser el listado de teléfonos de empresa o correos corporativos que tiene una empresa para la comunicación interdepartamental.
- Información restringida: Esta información es accesible solo por cierto personal dentro de la empresa, el cual lo necesita para la realización de su trabajo, un ejemplo de este tipo de información podrían ser las nóminas.

- Información confidencial: Esta información es la considerada de gran relevancia para el futuro de la empresa, por lo que solo tendrán acceso un número muy reducido de personas dentro de la empresa, esta información puede ser por ejemplo un proyecto futuro que tenga pensado realizar la empresa.

La información también puede ser clasificado siguiendo otros criterios, como su utilidad o el impacto que tendría su perdida, robo o destrucción.

Si la clasificamos según su utilidad deberíamos de ver a que hace referencia la información, de esta forma podremos clasificarla atendiendo a si es de clientes, proveedores, compras, ventas, personal, …

Si la clasificación la llevamos a cabo por el impacto de la perdida, robo o destrucción tendremos diferentes niveles dependiendo de la gravedad, los niveles serian el daño a la imagen, consecuencias legales, consecuencias económicas y paralización de la actividad.

En el departamento de Recursos Humanos el criterio que se debería de usar es el de confidencialidad. Esto es debido a que hay información que algunas personas del departamento deben de usar para el desempeño de su trabajo, que no debe de ser accesible para los demás, como las nóminas, el programa que utilizan para realizarlas o la información de los trabajadores, por ejemplo.

El uso del criterio del impacto que tendría su perdida, también se puede realizar, si bien la clasificación quedaría más incompleta, ya que el criterio de confidencialidad en cierto punto incluye el criterio del impacto de la perdida, robo o destrucción. Esto se debe a que, si una información es restringida o confidencial, una de las razones es el impacto de su robo, destrucción o perdida.

Para realizar una clasificación más completa se podría usar un sistema de clasificación que use tanto los criterios de confidencialidad como los del impacto de la perdida, robo o destrucción. Esta clasificación se realizaría primero atendiendo a la confidencialidad y posteriormente atendiendo al impacto.

Una vez clasificados se debe de etiquetar los activos de información. En el caso de que se encuentren en formatos digitales, un método puede ser añadir una etiqueta al comienzo del nombre del fichero, en el que se indique el nivel de confidencialidad y el de impacto. El nivel de confidencialidad indicará si es público, interno, restringido o confidencial. El nivel de impacto se indicará después del de confidencialidad, mediante un número, el cual hará referencia al tipo de impacto, siendo: 1 el daño a la imagen, 2 las consecuencias legales, 3 las consecuencias económicas y 4 la paralización de la actividad. Podrá darse más de un impacto, por lo que en caso de dos o más, se deberá de poner todos. Un ejemplo de este sistema de clasificación en formato digital es: [RESTRINGIDO 1-2]Nóminas_Enero_2020.xlsx o [CONFIDENCIAL 1-3]Proyecto_Marzo_2021.docx.

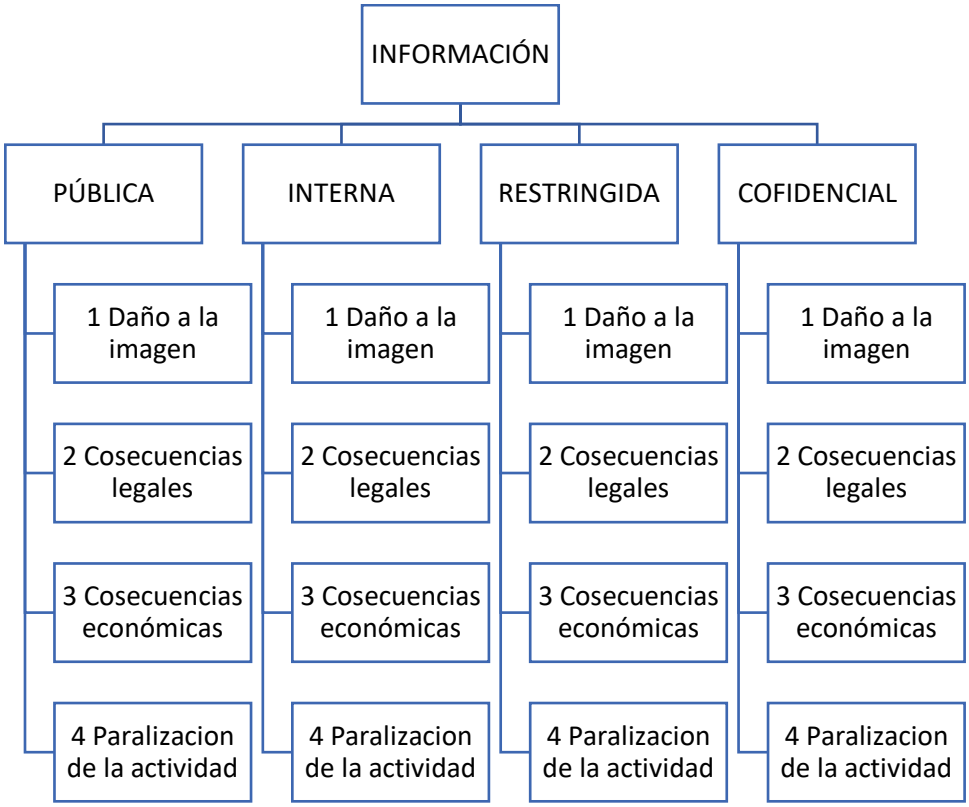

Figura 2 Esquema de la clasificación de la información en el departamento de Recursos Humanos

Para los activos en formatos físicos la etiquetación se puede realizar de diferentes maneras. Una puede ser el uso de archivadores diferentes para cada nivel de confidencialidad. Al mismo tiempo se pude usar adhesivos que indiquen la confidencialidad y el impacto, de esta forma nos aseguraremos de que sean correctamente almacenados.

Una vez clasificados los activos de información, se va a ver los diferentes medios y medidas de seguridad que se deben de realizar, siendo los más comunes el cifrado, las copias de seguridad y el control de acceso.

C. Seguridad en el tratamiento de datos (ciberseguridad)

Los encargados de tratar los datos de los trabajadores deberán de tener especial cuidado con la seguridad informática, debido a que se tratan datos especialmente sensibles.

Algunas de las medidas básicas de seguridad que deben de tomar están relacionadas con evitar que las personas puedan acceder físicamente a los datos, aunque algunas de estas medidas pueden parecer conocidas y obvias, muchas veces no se realizan de la manera correcta.

La mayor parte de las empresas afirman que la información es esencial para ellas, sin embargo, eso no se transmite a como tratan la seguridad de los datos. Y es que, *"en ocasiones se hace poco o muy poco para conservar y gestionar este auténtico patrimonio empresarial, dejando a la buena voluntad o a la evidente honradez de los miembros de la Entidad su utilización sin el debido control y sin tener en cuenta que lo que*

no ha pasado hasta el momento podría muy bien suceder en un minuto." (Ferrer Serrano, 2019, pág. 87). Esto se puede deber a muchos factores, por ejemplo, la falta de consciencia por parte de los trabajadores, que se puede manifestar en como guardan las contraseñas. Es muy habitual ver en las empresas que los trabajadores dejan en lugares visibles las contraseñas, por ejemplo, pegadas al marco del ordenador. Esto ocasiona que el uso de la contraseña sea totalmente ineficaz, ya que toda la seguridad que obtienes con su uso se pierde por ser visible para todos. Una de las formas de solucionar estos problemas en el uso de medidas de seguridad es dar a los trabajadores una formación general en seguridad informática. De esta manera se espera que se conciencien de la importancia que tiene para la empresa, además de conocer las medidas básicas de seguridad.

Algunas de las medidas básicas de seguridad son:

- Bloquear el ordenador con contraseña cuando el trabajador este ausente.
- No dejar apuntadas las contraseñas en papeles u otros medios de fácil acceso.
- No decir las contraseñas a otras personas.
- Usar contraseñas seguras.
- Cambiar las contraseñas cuando sean facilitadas de forma genérica.
- Implementar un acceso mediante *One Time Password* (OTP) o contraseña de un solo uso.

En el departamento de Recursos Humanos los equipos informáticos, como los ordenadores o los teléfonos móviles, por ejemplo, son una herramienta muy usada en el desarrollo de las funciones del departamento. Esto hace que en ocasiones se almacene cierta información en estos equipos, por lo que es necesario que exista en la empresa una política de seguridad en el almacenamiento de datos en la que se regule el almacenamiento en los diferentes dispositivos. Además, los trabajadores deberán de conocer esta política y estar concienciados de la importancia de su uso. Esta política deberá de tratar las diferentes medidas de seguridad que se deben de tener en cuenta cuando se usen los dispositivos, especificando las peculiaridades de cada uno. Además de los sistemas digitales deberá de tratar también los sistemas físicos.

En el apartado de la política referente a los equipos corporativos se deberá de establecer que información es susceptible de ser almacenada y cual no lo es. Los archivos personales del trabajador, como fotografías o archivos de música, no deben de ser almacenados en los equipos corporativos. En la política deberá de indicarse donde guardar cada tipo de información dentro del árbol de directorios del equipo, con la finalidad de facilitar la transferencia de la información a los servidores de la empresa. Así mismo, deberá de establecerse el tiempo de conservación de la información en los equipos, antes de decidir si se elimina o se transfiere a los servidores. En el caso de que la información se transfiera a los servidores, se deberá de establecer un periodo de permanencia en el equipo, tras el cual será eliminada para no tener duplicada la información almacenada. Con esto conseguiremos que los equipos no tengan gran cantidad de datos, al

encontrarse estos en el servidor, cuyo acceso es más complicado para las personas que carezcan de autorización.

Es habitual que la empresa cuente con servidores corporativos de almacenamiento en red, ya que este tipo de almacenamiento permite compartir información entre diferentes trabajadores de la empresa, además de permitir el almacenamiento de los trabajos realizados por cada trabajador. En este tipo de almacenamiento se debe de distinguir entre la información de trabajo y la información general de la empresa, la cual puede ser usada por todos los trabajadores. También es muy importante, como indica el INCIBE, que las políticas de seguridad y control de los accesos sean definidas por: la dirección y el responsable de sistemas. De esta forma se evitará que los trabajadores accedan a información que no deberían, como por ejemplo, que un trabajador de marketing acceda a las nóminas de los trabajadores. En el caso de que la empresa tenga varios servidores corporativos, el empresario deberá de realizar un listado de servidores corporativos, indicando la información que se puede almacenar en cada uno. Los servidores más usados para guardar gran cantidad de datos en las empresas son los de tipo *Network Attached Storage* (NAS), aunque dependiendo de la finalidad también se puede usar sistemas *Storage Area Network* (SAN) o sistemas *Direct Attached Storage* (DAS). Los sistemas DAS se diferencian de los NAS y los SAN en que el almacenamiento es local, en vez de remoto. La gran ventaja de estos sistemas es que aportan una gran cantidad de volumen de almacenamiento. Los servidores que tenga la empresa deberán de ser auditados cada cierto tiempo con la finalidad de revisar su estado, en cuanto a su capacidad, registros, parches de seguridad, etc.

Otra manera de almacenar información es en sistemas de almacenamiento en la nube. Este tipo de sistemas presenta aspectos positivos y negativos, los cuales deben de ser analizados antes de implantar estos sistemas en la empresa. Como aspectos positivos se pueden destacar: la capacidad de acceder a la información desde cualquier dispositivo y lugar, el menor coste económico frente a otros dispositivos o la posibilidad del trabajar varias personas sobre un mismo documento a la vez, entre otros aspectos positivos. Como aspectos negativos destacan la necesidad de conexión a internet o la dependencia de terceros. La empresa debería de elaborar un listado de servicios de almacenamiento en la nube permitido y prohibidos. Esto es importante debido a la existencia de servicios gratuitos que puede que no aporten la seguridad necesaria. También se deberá de incluir en la política de seguridad que información puede ser almacenada en estos servicios y el proceso para eliminarla. Previamente a la contratación de un servicio de este tipo se deberá de ver si la política de seguridad del proveedor cumple con las necesidades que se tienen. La seguridad del servicio debe de ir acorde a la información que se pretende depositar.

En cuanto a los dispositivos extraíbles como: memorias USB, discos duros portátiles o tarjetas de memoria. Los cuales permiten transferir de forma rápida y directa información, es necesario que en política de seguridad de la empresa se establezca como deben de ser usados estos dispositivos. Así mismo, los empleados deberán de estar concienciados de cómo usar estos dispositivos. Hay que tener en cuenta que

algunos son muy usados y en ciertos casos imprescindibles, además sus características hacen que sean susceptibles de ser robados, extraviados, manipulados o infectados por un virus.

En esa política se deberá de establecer: si está permitido su uso o no, en que situaciones se puede usar y que información se puede guardar, si está permitido el uso de dispositivos personales, que medidas de seguridad se deben de realizar o cómo se deben de eliminar los datos almacenados.

Algunas de las medidas de seguridad que se pueden establecer en la política en cuanto al uso de dispositivos extraíbles son: el cifrado de los datos que se almacenen, el uso de contraseñas y su cambio periódicamente o establecer permisos de acceso. A la hora de eliminar los datos almacenados se debe de tener en cuenta la clasificación de la información que contiene, dependiendo de la cual, se eliminará de una u otra manera. Algunas formas de eliminar los datos de los dispositivos extraíbles para que estos no vuelvan a ser accesibles son: la destrucción física, la desmagnetización o la sobreescritura. Se elegirá que método usar dependiendo del caso.

Cuando se usen dispositivos extraíbles para almacenar información confidencial o especialmente sensible, se deberán de utilizar dispositivos corporativos que estén protegidos, así mismo su almacenamiento deberá de ser en un lugar seguro. Cuando ocurra algún incidente, como pérdida o robo, con estos dispositivos se deberá de informar al responsable de sistemas o de seguridad informática inmediatamente.

En la política de seguridad la empresa deberá de tener en cuenta el uso de dispositivos móviles, como portátiles, *tablets* o teléfonos móviles. Estos dispositivos presentan la ventaja de tener una gran movilidad, permitiendo al trabajador tener acceso a aplicaciones corporativas, correo corporativo o información confidencial, por ejemplo. Esto ocasiona que el trabajador pueda trabajar como si estuviera en las instalaciones de la empresa, pero sin estarlo. Esta ventaja puede ser de gran utilidad en el caso de trabajadores con viajes de empresa o para casos excepcionales, como la pandemia del Covid-19, que obligan a los trabajadores a teletrabajar. La gran movilidad de estos dispositivos implica que estén expuesto a mayores riesgos de pérdida o robo, por lo que es necesario tomar ciertas medidas de seguridad para evitar que un acceso no autorizado a la información de la empresa. Algunas de las medidas de seguridad que se deben de tomar son: contraseñas de acceso seguras, cifrar la información que almacenen, mantener el antivirus activo, mantener el equipo actualizado, etc.

En la política de seguridad se deberá de establecer si está permitido el uso de dispositivos propios de los trabajadores. En caso de que este permitido se deberá de establecer las medidas de seguridad para estos dispositivos, así como los supuestos en que está permitido su uso.

El uso de dispositivos propios de los trabajadores presenta un mayor riesgo que el uso de dispositivos móviles corporativos. Esto se debe a que los dispositivos propios se encuentran expuestos a: redes inseguras en el ámbito personal, instalación de aplicaciones que puedan suponer un riesgo para la información almacenada, la falta de antivirus o de actualizaciones, un mal uso de los medios de control de acceso, etc.

En cuanto a los dispositivos corporativos hay que llevar un registro sobre los trabajadores que los tienen. Los que usen estos dispositivos deben de tener prohibido hacer cambios en el hardware o instalar software, cuando no estén autorizados para ello, cuando se conecten a redes ajenas a las de la organización deberán de seguir el protocolo de la empresa para estas conexiones. En caso de que el trabajador sospeche que el dispositivo está infectado por un virus o software malicioso deberá de comunicarlo al personal técnico. Así mismo cuando el dispositivo se encuentre fuera de la empresa el responsable de su seguridad será el trabajador.

Aunque las empresas almacenan la mayor parte de la información en formatos digitales, todavía es habitual que algunos datos se encuentren en formatos físicos. Por lo que la política de almacenamiento de datos deberá de contar con un apartado sobre este tipo de información, en el que especifique cómo y dónde debe de ser almacenada. En el caso de información de carácter público es probable que sea suficiente con almacenarla en archivadores o armarios, pero si se trata de información con un carácter más confidencial lo lógico es que esta deba de ser guardada en un lugar más seguro. Dependiendo de la confidencialidad se podrá usar, por ejemplo, un archivador con llave, una sala segura con acceso restringido o una caja fuerte.

Medidas de seguridad

Como se ha visto anteriormente es importante que se establezcan medidas de seguridad y que se disponga, en la política de seguridad, en que supuestos se deberá de usar cada medida. A continuación, se va a indicar algunas medidas que son consideradas importantes para mantener la información segura en el departamento de recursos humanos. Las medidas básicas de seguridad de las que se habló anteriormente, al igual que las medidas de las que se hablará a continuación, deberán de encontrarse detalladas en una parte de la política de seguridad, o en un manual corporativo dedicado exclusivamente a ellas. Además, se deberá de formar a los trabajadores para que sepan cómo aplicarlas correctamente, ya que el simple hecho recogerlas por escrito no es suficiente debido a que los trabajadores pueden no comprender correctamente como, cuando y de qué forma deben de aplicarlas.

Una de las medidas para mantener segura la información es el control de acceso. Consiste en limitar quién puede acceder, cómo puede hacer, cuándo puede acceder y con qué finalidad puede acceder. En la empresa habrá un encargado de conceder o revocar los permisos, los cuales deberán de ser revisados periódicamente para comprobar que son los correctos. También deberá de eliminar los permisos de los trabajadores que dejen de prestar servicios en la empresa, para evitar que puedan sustraer, eliminar o modificar información.

Otra medida para mantener segura la información y protegerla en caso de un incidente es la realización de copias de seguridad. La empresa deberá de tener un responsable de realizar las copias de seguridad. Además, deberá de contar con un procedimiento que indique cómo realizar las copias de seguridad y restaurarlas, el cual tendrá que incluir: los archivos de los que realizar la copia de seguridad, el tipo de copia,

el programa con el que realizaran, la periodicidad, la vigencia, los soportes y la ubicación. El responsable deberá llevar un control de los soportes usados, quién tiene acceso y la forma de destruirlos. Esta medida es muy importante realizarla debido a que, aunque no es muy habitual, puede suceder que el dispositivo que contenía la información sufra un fallo o accidente que ocasione su destrucción o la perdida de la información que contenía. Por ello la existencia de copias de seguridad puede resultar vital para recuperar la mayor parte de la información, minimizando los daños.

Una de las grandes amenazas a la que hacen frente las empresas, como indica el INCIBE en su Guía de almacenamiento seguro de la información (Instituto Naconal de Ciberseguridad), son los virus y otros tipos de *malware* existentes, así como los nuevos que aparecen. Para proteger la información de estas amenazas la empresa deberá de contar con un apartado que les haga referencia en la política de seguridad o con una política de control de *malware*. Esta deberá de incluir como hacerles frente, además deberá de revisarse periódicamente para evitar su obsolescencia. El tipo de solución que se deberá de implantar en la empresa dependerá del tamaño, el nivel de seguridad que es necesario y la complejidad de las configuraciones. Podemos diferenciar dos grupos de soluciones: las soluciones globales corporativas y las herramientas para el puesto de trabajo o dispositivos de trabajo.

Algunas herramientas de seguridad contra el *malware* son: los *antiphishing*, los antimalware, los antivirus o los antispam, por ejemplo. Las herramientas que se usen deberán de estar configuradas correctamente y mantenerse actualizadas para que la seguridad sea la adecuada y sean eficientes. La empresa deberá de tener un procedimiento de respuesta ante infecciones causadas por un *malware*. También se deberá de mantener concienciada a la plantilla sobre los peligros del *malware*, para lo que la empresa deberá de contar con una política de buenas prácticas para prevenir infecciones de *malware*. Esta política deberá de prohibir la ejecución de ficheros descargados de servidores externos o soportes no autorizados. El correo deberá estar configurado para no ejecutar automáticamente los correos, además los trabajadores no podrán modificar la configuración de seguridad de los dispositivos y deberán de usar los softwares autorizados por la empresa. Todas los contenidos y descargas deberán de considerarse potencialmente inseguros hasta que sean analizados por una herramienta antimalware.

El *phishing* es uno de los principales motivos de brecha de seguridad en las empresas. Esta amenaza consiste en que un estafador engaña a la víctima usando técnicas de ingeniería social, normalmente se gana la confianza haciéndose pasar por otra persona o empresa. Aparentemente puede parecer que se trata de una comunicación oficial, por el contrario, no es así. De esta forma el estafador puede obtener información sensible de la empresa, por lo que es muy importante que se usen herramientas *antiphishing* y que esta amenaza sea incluida en la política de seguridad.

La realización de estas acciones, junto con las que veremos a continuación, no garantiza que no pueda infectarse un equipo, pero sí que reduce estos riesgos de forma muy importante, al tratar las formas habituales de infección.

El software que se use en la empresa deberá de mantenerse actualizado, esto se debe a que cuando el fabricante del software lanza una actualización o parche es porque añade o mejora las funciones, o porque ha detectado un error o agujero de seguridad y lo está solucionando. En caso de que no actualicemos el software podríamos estar exponiendo el dispositivo a todo tipo de riesgos, incluso el robo de datos e información confidencial de la empresa. En el caso de que el software tenga la función de actualizarse automáticamente debería de estar activada, para la actualización manual de los softwares que no cuentan con versión automática, se deberá de obtener el software de un lugar de confianza. También hay que tener en cuenta el ciclo de vida de los softwares, ya que, si queda obsoleto y no cuenta con soporte oficial del fabricante, supondrá que el software es vulnerable a ciberdelincuentes, por lo que el software deberá de dejarse de usar en la empresa. La empresa deberá de llevar un registro de los softwares y las actualizaciones que se han instalado en sus sistemas.

Otra medida para mantener la información confidencial o de carácter personal segura es cifrarla. Así mismo, es recomendable cifrar el disco de arranque, los discos duros internos y extraíbles, el correo, las copias de seguridad, los dispositivos móviles, los ficheros y los directorios. Los sistemas de cifrado que se usen deberán de estar vigentes y si es posible es preferible que sea de cifrado asimétrico en vez de simétrico. Con esta medida se logrará que, en caso de que alguien obtenga acceso a los dispositivos que contienen la información, este no pueda acceder al contenido de la información de forma fácil. El cifrado de la información presenta grandes ventajas de seguridad. Debido a esto se deberá de usar cuando se envié por correo electrónico información sensible, ya que en caso de que un ciberdelincuente tuviera acceso al correo, no tendría acceso a la información al carecer de la clave de cifrado. Otra ventaja es la de dificultar el acceso a la información cuando un dispositivo se pierde o es sustraído. El uso de esta medida debería de tener carácter obligatorio para la información confidencial o sensible, de acuerdo con lo expuesto anteriormente.

A continuación, se va a tratar aspectos que se deben de tener en cuenta en el uso de credenciales de autenticación. Estas están formadas por un usuario y una contraseña, lo habitual es que cuando un trabajador accede a la empresa se le facilite una pareja de credenciales. Por ejemplo, al nuevo integrante del departamento de recursos humanos se le facilitara unas credenciales que permitan su acceso a los ficheros del departamento. Pero hay que tener cuidado, ya que lo habitual es que la contraseña sea genérica, por lo que deberá de cumplir con las medidas básicas expuestas con anterioridad, incluida la de cambiar la contraseña. Al trabajador le puede surgir la duda de que contraseña establecer, para que esta sea segura, por eso a continuación se van a dar unas pautas para el establecimiento de una contraseña.

La nueva contraseña deberá de tener 8 o más caracteres, no deberá de ser apodos, números de teléfono, fechas de cumpleaños u otros datos personales fáciles de averiguar. Tampoco deberá de ser palabras, frases o patrones comunes, como podrían ser “contraseña”, “abcd” o “12345”. Deberán de contar con al menos un número, una letra en mayúscula y un símbolo (por ejemplo: ¿, /, %), de esta forma se establecerá una contraseña segura. Ahora bien, establecer una contraseña segura no servirá de nada si se escribe en papel y se deja en un lugar visible. En el caso de que el trabajador necesite tener la contraseña anotada deberá de guardarla bajo llave o en un lugar secreto que garantice que solo él puede acceder.

El uso de todas estas medidas, tanto en la empresa, como en el departamento de Recursos Humanos, resulta importante para garantizar la seguridad de la información. Como se expuso anteriormente, supone un activo muy importante para las empresas, por lo que deben de gozar de ese estatus en lo referente a su tratamiento y seguridad.

V. Conclusiones

A lo largo del trabajo he podido analizar cómo debe de tratarse la protección de datos, he visto la protección que se le da en la legislación, tanto en la Unión Europea, como en España. De este análisis he podido descubrir que la protección de datos engloba unos derechos que se ven afectados por la evolución tecnológica. Dándose la situación de que la legislación deba de adaptarse con el tiempo a estos avances tecnológicos, ya que de lo contrario puede suceder que algunos derechos que tienen las personas, como el derecho a la intimidad, queden desprotegidos. En el caso de España considero que el tiempo transcurrido desde la Ley Orgánica 15/1999 hasta la Ley Orgánica 3/2018, es excesivo. Ya que, durante ese tiempo, por ejemplo, los trabajadores no tuvieron una regulación propia de los derechos digitales en el ámbito laboral, quedando la protección de sus derechos condicionada a lo que se establecía judicialmente.

Otra conclusión que he sacado es que el personal de recursos humanos de las empresas debe de conocer la legislación en materia de protección de datos, así como conocer cómo deben de tratar los datos. Durante mi experiencia en un departamento de Recursos Humanos he podido observar que cada vez se da mayor importancia a la protección de datos. Sin embargo, no todas las empresas aplican la protección de datos de forma adecuada. Las empresas, desde mi punto de vista, deben de formar a los trabajadores del departamento de Recursos Humanos en tratamiento y protección de datos. Esta formación debería de estar en consonancia a las medidas y políticas de protección de datos que, desde mi parecer, deben tener las empresas.

Considero que las empresas deberían de revisar periódicamente sus políticas y medidas de protección de datos, ya que, como comenté anteriormente la evolución tecnológica es muy rápida, lo que ocasiona que lo que hoy es una medida de seguridad de validad, en un futuro puede no serlo. Esto hace que la protección de datos sea una materia en continua evolución, a la cual hay que mantener en constante escrutinio.

Creo que las empresas que cuenten con una cantidad de trabajadores considerable deberían de aplicar y obtener los certificados de las normas ISO. Esto ayudaría a la empresa en materia de protección de datos, provocando que sea más sencillo adecuarse a los cambios que surjan durante su evolución. Además, el hecho de obtener las certificaciones será beneficioso para la empresa, ya que demostrará a sus trabajadores y al exterior que la empresa se preocupa por la protección de sus datos. Esto la hace más atractiva para posibles futuros aspirantes a trabajar en la empresa, así como para los clientes y proveedores.

Finalmente, considero que el personal de Recursos Humanos debe de clasificar los datos atendiendo, como mínimo al criterio de confidencialidad. De esta forma conseguirán, si se aplican las medidas de seguridad que corresponden para cada nivel, que los datos tengan una seguridad adecuada. La clasificación de la información tiene la finalidad de facilitar la aplicación de las medidas de seguridad. Creo que un correcto sistema de clasificación, pudiendo ser el que propongo u otro, ayuda a reducir el tiempo que se debe destinar

a mantener seguros los datos. De esta forma se conseguirá que el departamento de Recursos Humanos sea más eficiente en el tratamiento de datos.

VI. Bibliografía

Agencia Española de Protección de Datos. (2019). *Novedades Ley Orgánica 3/2018 para el sector privado.* Obtenido de https://www.aepd.es/sites/default/files/2019-10/novedades-lopd-sector-privado.pdf

Ferrer Serrano, R. (2019). *Guía de protección de datos de los trabajadores.* (1º ed.). Valencia: Tirant lo Blanch.

Instituto Nacional de Ciberseguridad. (2018). *Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario.* Obtenido de https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

Instituto Nacional de Ciberseguridad. (s.f.). *Políticas de seguridad para la pyme.* Obtenido de https://www.incibe.es/protege-tu-empresa/herramientas/politicas

Instituto Naconal de Ciberseguridad. (s.f.). *Guía de almacenamiento seguro de la información.* Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

International Organization for Standardization. (2013). *ISO/IEC 27001:2013* (2º ed.).

International Organization for Standardization. (2013). *ISO/IEC 27002:2013* (2º ed.).

International Organization for Standardization. (2019). *ISO/IEC 27701:2019* (1º ed.).

Microsoft. (2020). *Ley de privacidad del consumidor de California (CCPA)*. Obtenido de https://docs.microsoft.com/es-es/microsoft-365/compliance/offering-ccpa?view=o365-worldwide

Muñoz Machado, S. (2015). *Los tres niveles de garantías de los derechos fundamentales en la Unión Europea: problemas de articulación.* Madrid: Revista de Derecho Comunitario Europeo, núm. 50.

Orellana Cano, A. (2019). *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores.* (1º ed.). Cizur Menor (Navarra): Aranzadi.

Preciado Domènech, C. (2017). *El derecho a la protección de datos en el contrato de trabajo.* Navarra: Aranzadi.